Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Currently Amended) A method of providing a secure data stream between system nodes, the method comprising:

~~encrypting data at a node with an encryption key;~~

providing a data record block including a plurality of data records encrypted within a predetermined time interval;

providing a previous encryption key;

selecting ~~encrypted data~~ an old data record from the plurality of data records; and

regenerating a new encryption key at a user node ~~with an~~ as a function of the previous encryption key and ~~selected encrypted data~~ the old data record.

2. (Currently Amended) The method of claim 1 wherein the step of selecting ~~encrypted data~~ the old data record comprises selecting ~~encrypted data~~ the old data record using a byte from [[a]] the previous encryption key as a seed of random generation.

3. (Currently Amended) The method of claim 1 wherein the step of regenerating [[a]] the new encryption key comprises regenerating a new encryption key by performing a logic operation on [[a]] the previous encryption key and ~~selected encrypted data~~ the old data record.

4. (Currently Amended) The method of claim 3 wherein the step of regenerating [[a]] the new encryption key by performing a logic operation comprises regenerating [[a]] the new

encryption key by performing an XOR logic operation on [[a]] the previous encryption key and ~~selected encrypted data~~ the old data record.

5. (Currently Amended) The method of claim 3 wherein the step of regenerating [[a]] the new encryption key by performing a logic operation comprises performing [[a]] the logic operation on [[a]] the previous encryption key and ~~selected encrypted data~~ the old data record to form an expanded key.

6. (Currently Amended) The method of claim 5 further comprising the step of selecting bytes from [[an]] the expanded key to generate the new encryption key.

7. (Currently Amended) The method of claim 6 wherein the step of selecting bytes from [[an]] the expanded key to generate the new encryption key comprises randomly selecting bytes from [[an]] the expanded key to generate the new encryption key.

8. (Currently Amended) The method of claim 7 wherein the step of randomly selecting bytes from [[an]] the expanded key to generate the new encryption key comprises randomly selecting bytes from [[an]] the expanded key using a byte from [[a]] the previous encryption key as a seed of random generation.

9. (Currently Amended) The method of claim 1 further comprising the step of encrypting [[data]] a new data record with [[a]] the new encryption key forming a new encrypted data record.

10. (Currently Amended) The method of claim 9 wherein the step of encrypting [[data]] the new data record with [[a]] the new encryption key comprises performing a logic operation on the [[data]] new data record and the new encryption key.

11. (Currently Amended) The method of claim 10 wherein the step of performing a logic operation on the [[data]] new data record and the new encryption key comprises performing an XOR operation on the [[data]] new data record and the new encryption key.

12. (Currently Amended) The method of claim 10 wherein the step of performing a logic operation on the [[data]] new data record and the new encryption key comprises forming a cipher.

13. (Original) The method of claim 12 further comprising the step of permuting portions of the cipher to form another cipher.

14. (Currently Amended) The method of claim 9 further comprising the step of transmitting ~~encrypted data~~ the new encrypted data record over a data stream.

15. (Currently Amended) The method of claim 14 further comprising the step of receiving ~~encrypted data~~ the new encrypted data record at a destination node.

16. (Currently Amended) The method of claim 15 further comprising the step of decrypting ~~encrypted data~~ the new encrypted data record at the destination node.

17. (Currently Amended) The method of claim 16 wherein the step of decrypting ~~encrypted data~~ the new encrypted data record comprises decrypting the new encrypted data record with a previous decryption key forming a new decrypted data record.

18. (Currently Amended) The method of claim 17 further comprising the step of regenerating a new decryption key ~~using selected decrypted data~~ as a function of the new decrypted data record and [[a]] the previous decryption key.

19. (Currently Amended) A system for providing a secure data stream between a source programmable apparatus and a destination programmable apparatus, the system comprising:

a source programmable apparatus;

a data stream created by said source programmable apparatus;

means for encrypting [[data]] a data record of said data stream with [[an]] a previous encryption key forming an encrypted data record; and

means for regenerating a new encryption key using selected ~~previously encrypted data~~ as a function of the previous encryption key and an old data record.

20. (Currently Amended) The system of claim 19 further comprising:

a destination programmable apparatus in ~~electrical~~ communication with said source programmable apparatus;

means for transmitting ~~encrypted data~~ the encrypted data record to said destination programmable apparatus;

means for decrypting said ~~encrypted data~~ the encrypted data record received at said destination programmable apparatus with a previous decryption key forming a decrypted data record; and

means for regenerating a new decryption key ~~using selected previously decrypted data~~ as a function of the previous decryption key and the decrypted data record.